Proceedings of the 2024 Winter Simulation Conference
H. Lam, E. Azar, D. Batur, S. Gao, W. Xie, S. R. Hunter, and M. D. Rossetti, eds.

IS SYSTEMIC CYBER RISK MANAGEMENT FOR ENTERPRISES SUSTAINABLE?

Ranjan Pal[1], Konnie Duan[1, 2], Rohan Xavier Sequeira[3] and Michael Siegel[1]

[1]MIT Sloan School of Management, Massachusetts Institute of Technology, Cambridge, MA, USA
[2]Department of EECS, Massachusetts Institute of Technology, Cambridge, MA, USA
[3]Electrical and Computer Engineering, University of Southern California, Los Angeles, CA, USA

ABSTRACT

Business enterprises have grappled in the last one and half decade with unavoidable risks of (major) cyber incidents. The market to manage such risks using cyber insurance (CI) has been growing steadily but is still skeptical of the economic and societal impact of systemic risk across networked supply chains in interdependent IT-driven enterprises. While systemic risk from traditional cyber loss events might lure more capacity to the CI market, such a risk from a catastrophic (CAT) cyber loss event can quite likely reverse this trend. The sustainability of the much viable risk diversification by cyber insurers in these environments depends on (a) the statistical nature of cyber risks that contribute to systemic cyber risk and (b) the interconnection topology between enterprises. We focus here on (a) and solve the theory challenge problem of proposing simulation-validated mathematical conditions on cyber risk distributions that make systemic risk VaR diversification-friendly for CI markets.

1 INTRODUCTION

The cyber insurance market as a third party market to manage enterprise cyber risk has seen a significant growth rate in the last five years in the USA (greater than 50% annually since 2020 according to *Conning*, an investment management firm for the insurance industry) and in many other countries around the globe. Most of it is due to the spike in ransomware claims since 2019 (based on a survey by insurance analytics firm *NetDiligence* in 2023) that has allowed cyber insurers to write higher premiums on a narrow exposure base with tightened exclusionary policies. Such policies have usually enforced that enterprises adhere to strictly recommended security controls (e.g., MFA, strong passwords) for attractive premiums and/or the necessary condition to get insurance coverage. A recent survey by *Forrester* in 2023 provided statistics showing that such security controls necessitated on enterprises by standalone cyber insurance policies reduced (when compared to non-standalone policies) the number of cyber incidents involving data breaches and also improved cyber resilience by reducing the mean time to incident detection, response, and recovery.

However, this growth rate can only be sustained, not by writing further higher premiums for narrow exposures, but by more enterprises resorting to cyber insurance. In other words, the big supply-demand gap in the current cyber insurance industry running in atleast hundreds of billions of USD will need to be closed in. While in the environments of scales of loss impact that we have seen till date, it is likely that the cyber insurance business will continue to grow steadily to say the least. However, it is common knowledge that the cyber risk terrain is extremely dynamic and expansive; hence it is unlikely to believe that this evolving terrain would be perennially growth-friendly for the non-predictable and new cyber insurance market (in contrast to the traditional insurance markets) where the insurers usually have low historical data and model confidence to accurately estimate the economic and societal impact of a wide variety of cyber attacks. To drive home this point, ransomware-as-a-service that started around 2014 hardly used to exceed multiple thousands of USD until 2019, when suddenly nation state actors demanded multi-million dollars on a single ransomware incident or from a systemic impact of a single incident. Such impact spikes are extremely difficult to predict using historical data. Add to this that systemic events such as a catastrophe

loss event (including those larger than any we have seen till date) could very likely and unpredictably reverse the trend of cyber insurance markets growing on narrow exposure bases in the aftermath (e.g., the 2018 NotPetya cyber attack impact that initially pushed leading cyber insurers to opt out of providing demanded coverage amount).

The systemic economic and societal impact of adversaries exploiting this evolving and expanding cyber terrain is much amplified in the IT-driven enterprise ecosystem that subsumes (apart from large enterprises) small and medium business (SMB) sectors that are usually interdependent, networked, and form the majority of the businesses around the globe. Such enterprises that form an integral part of multiple enterprise supply chain networks are usually (traditionally) not that vigilant about adopting a strong cyber hygiene but nonetheless fear about cyber attacks impacting their businesses, and present a huge uncovered cyber risk exposure to insurers and reinsurers. Under such situations and target victim space, it is not clear whether the cyber insurance and reinsurance businesses will be sustainable and scale as per the needs of enterprises and society and 'enforce' sufficient security controls to improve cybersecurity of the enterprise ecosystem. *In this paper, we are interested/motivated in mathematically solving for the conditions that guarantee the existence of sustainability of systemic cyber risk management in IT-driven enterprise ecosystems by cyber insurers and reinsurers.* In the rest of the section, we first showcase through examples why systemic cyber risk is a very important near futuristic problem for enterprise cyberspace. We then present the motivational challenges of our research. Finally, we propose the research contributions.

1.1 Why is Systemic Cyber Risk Management an Important Problem for Insurers and Enterprises?

In this section, we showcase the importance of cyber risk management for insurers and enterprises in a connected ecosystem.

We first provide the definition of systemic cyber risk as put forward by the World Economic Forum in 2016 (Hanouz 2016). *"Systemic cyber risk is the risk that a cyber event (attack(s) or other adverse event(s)) at an individual component of a critical infrastructure ecosystem will cause significant delay, denial, breakdown, disruption or loss, such that services are impacted not only in the originating component but consequences also cascade into related (logically and/or geographically) ecosystem components, resulting in significant adverse effects to public health or safety, economic security or national security. The adverse real economic, safety and security effects from realized systemic risk are generally seen as arising from significant disruptions to the trust in or certainty about services and/or critical data (i.e. the integrity of data), the disruption of operations and, potentially, the incapacitation or destruction of physical assets."*

According to this definition, systemic cyber risk effects on economy and society could be of medium to a very large scale. Systemic cyber risk could usually either be from a *cascading failure* where a single cyber incident (i.e., a data breach, or loss of availability via service disruption) can propagate outward from an enterprise and disrupt businesses in many enterprises interconnected through supply chains, or from a *common cause cyber failure* where a single cyber exploit triggered at multiple enterprises result in multiple simultaneous cyber incidents (Welburn and Strong 2022). We list existing and potential real world scenarios of such impact scales and through the examples showcase the importance of cyber risk management for insurers and enterprises in a connected ecosystem.

1.1.1 Existing and Potentially Future Systemic Cyber Attacks

In the last three years there have been cascading failure attacks related to cloud outage (e.g., due to a data streaming analysis tool misconfiguration), email security provider failure (e.g., due to digital certificate compromised by foreign actors), and data aggregator software breach (e.g., due access gained through hardware redundancy failure). While in the case of the cloud outage and email security cyber attacks thousands of online service users (end users and enterprises) were systemically affected, millions of customers were affected due to the data aggregator software breaches. In the same three year period, there have been common cause failure attacks related to software supply chains (e.g., Log4J, SolarWinds

and Solorigate) and server infiltration (e.g. Hafnium). Software supply chain attacks happened due to the exploitation a major bug in the trusted software of major and IT network vendor used by multiple enterprises worldwide. The challenge to detection here is that bugs within packaged software in production environments, files (e.g., Java files as in Log4J) can be nested deep into other files that evades detection. Server infiltration attacks happened due to either a zero-day exploit or a severely known vulnerability exploit that allowed adversaries gain access through web-facing email exchange servers. Overall, according to *Chubb*, between 2020 and 2022, approximately 200K enterprises worldwide, both large and SMBs, were systemically affected on a low/medium scale.

The above type of cyber attacks were economically costly without a doubt but could have had a multiplicative effect if the adversary intent was to steal or destroy critical data. As said by Kevin Mandia, CEO of cybersecurity firm FireEye, in testimony to the Senate Intelligence Committee *"the threat actors behind the Solorigate attack had the access required and the capability required should they have wanted to be disruptive".* In other words, the above mentioned cyber attacks had a non-catastrophic systemic effect on the economy and society. In contrast, the NotPetya cyber attack (often termed as the worst cyber attack in history by multiple governments around the globe) that exploited M. E. Doc a tax software tool and spread the malware indiscriminately to a large number of enterprises in the USA, Europe, and other parts of the globe. NotPetya was actually a wiperware, not ransomware, aimed to destroy the data rather than hold it hostage for financial gain. It worked through threat actors creating a backdoor inside M. E. Doc disguised as a software update from compromised M. E. Doc servers. This large scale systemic spread resulted in a net estimated cyber loss of USD 10 billion across the enterprises with some individual enterprises accruing a loss exceeding USD 100 million.

NotPetya, as many believe, is the start of the tip of the iceberg of catastrophic systemic cyber attacks in the sense of the term. In a recent article (Eling et al. 2023), the authors proposed multiple futuristic realistic scenarios of catastrophic cyber attacks with a large scale impact on the economy and the society when compared to the events discussed above generating low/medium scale systemic impact. The attacks include (a) extortion of SCADA networks in critical infrastructure with an estimated mean economic impact (MEI) of USD 23 billion, (b) cloud service provider failure with an estimated MEI of USD 15 billion, (c) cyber attack on the health sector with an estimated MEI of 30 billion, (d) impairment of Internet communications with an estimated MEA of USD 1.5 billion, (e) cross-sector IT failure due to a cyber attack with an estimated MEA of 35 billion USD, (f) widespread data loss from an operating system with an estimated MEA of USD 23 billion, (g) large-scale data loss from a cloud service provider with an estimated MEA of USD 23 billion, and (h) a cyber attack on the US power grid with an estimated MEA of USD 50 billion.

1.1.2 The Challenge and Importance of Managing Systemic Cyber Risk

RiskRecon, a security analytics company acquired by *Mastercard* in 2019 made the following key findings on multi-party cyber risk in 2023: (i) more than 80% of IT driven global enterprises have recurrent third party connections, (ii) around 88% of these enterprises' vendor relationships extend to the 8th party, (iii) approximately 75% of business relationships occur at the 4th and 5th party levels, (iv) around 61% of an enterprise's 4th parties are relied upon by multiple 3rd parties, and (v) 21% of third parties have experienced a cybersecurity breach within the last three years.

Challenge - It is then evident then that with (a) the huge vulnerable cyber-terrain spanning the huge ecosystem of (Nth party) interdependent, geographically diverse IT-driven enterprises, and (b) a significantly growing supply chain built upon software, application, and hardware reliance via the cloud and the network of SMBs, we are looking a future with systemic/aggregate cyber loss impact distributions uniformly spread across the spectrum of various statistical 'shapes' (types) that might be exposed to cyber (re-)insurers. *These cyber loss distribution types will be have to be evaluated mathematically for cyber risk diversification (an integral job of insurance companies to manage risk over time and space) feasibility as a necessary condition for sustainable cyber risk management for enterprise ecosystems. Diversification feasibility is synonymous to the economic viability for the cyber (re-)insurers to sustainably manage*

systemic cyber risk over time and space. Only after this exercise (acting as a pre-requisite condition) can the cyber (re-)insurance industry address the other important challenges of case-dependent (depending on the diversification feasibility classification) cyber risk modeling and collecting sufficient data to attractively price CI (includes re-insurance) contracts for the client base. *Such an important mathematical exercise has been an open challenge in the cyber insurance research community till date* (see Section 6).

Importance - This diversification sustainability exercise is dependent upon the nature of the systemic cyber risk distributions alongside the interconnection topology of IT driven enterprises - factors that will drive the research on this problem. It is imperative that cyber insurers have a way out to ensure coverage market sustainability for all combinations of distribution statistics and enterprise network topologies to (a) avoid incurring high opportunity costs (that is currently the status quo) in the huge multi-trillion dollar cyber market - *showcasing the importance of market sustainability to the CI business*, (b) narrowing in the multi-billion dollar supply demand gap in the CI market, and (c) consequently, significantly boost social welfare via improved enterprise ecosystem cybersecurity through optimal cyber insurance controls - *showcasing the importance of market sustainability to improved enterprise cybersecurity.*

1.2 Research Contributions

In this paper, we primarily focus on the diversification sustainability exercise for systemic cyber risk management by only accounting for the statistical nature of systemic cyber risk distributions. More specifically, we make the following research contributions in this paper.

- We propose (to the best of our knowledge) the first mathematically rigorous classification scheme on the sustainability existence of systemic cyber risk management via the process of portfolio diversification in the CI industry (includes re-insurers), for general (i.i.d. and non i.i.d.) systemic cyber risk distributions based on their tail nature (see Sections 3 and 4).
- Our proposed classification theory is built upon the seminal *majorization theory* in the decision sciences and *statistical copula theory* in multivariate statistics. Our classification theory states whether a certain portfolio of (aggregate) cyber risk distributions on a(re-)insurance company's plate is diversification-friendly with respect to the dynamics of the industry-popular Value-at-Risk (VaR) measure with increasing portfolio size (see Sections 3 and 4). In theory, one of our *our main results states that a portfolio of (non) i.i.d. cyber risk distributions that are either light or heavy tailed with a finite mean can always be diversified in a sustainable manner, whereas a portfolio of (non) i.i.d. extremely heavy tailed cyber risk distributions cannot be sustainably diversified.* In scenarios when for a certain cyber risk distribution portfolio type consisting of non i.i.d. and i.i.d. distributions with heavy-tails with infinite mean and variance (examples being a portfolio of catastrophic systemic loss distributions), we propose a practical cyber risk sharing solution for cyber (re-)insurers, backed by mathematical guarantees, to make systemic cyber risk management for such risks sustainable (see Section 4). In particular *a main result of our proposed theory is that a large insurance market with many coordinating cyber insurers to share risk is sufficient to reduce the VaR of the shared portfolio of an insurer's cyber risk when compared to the VaR when the latter insurer absorbs the entire risk it is exposed to.*
- We run large scale Monte Carlo simulations to test our proposed theory in Section 3. Our simulations showcase interesting and market viable cyber risk diversification trends for *non i.i.d.* risks that will act as key insights to (re-)insurers to scalably manage the nature of systemic cyber risks that might actually be exposed to in practice (see Section 5).

This work only addresses the open challenge of ensuring sustainable systemic cyber risk management from a risk distribution viewpoint. The open challenge of jointly accounting for the statistical properties of these distributions along with the topological interconnectivity nature among enterprises to analyse systemic cyber risk management sustainability will be addressed as future work.

2 PRELIMINARY BACKGROUND

In this section, we provide the necessary mathematical background, including the definition of Value-at-Risk (VaR) - a commonly used industry risk measure, the class of mathematically stable distributions, and the basics of *majorization theory* (Marshall et al. 1974) which is essential to our analysis. *The preliminary background information overlaps with the background information in our previous work (Pal et al. 2020), and we borrow it for the purpose of continuity and notational consistency.*

2.1 The Value at Risk (VaR) Measure

Given a risk tolerance q, $0 \leq q \leq 1$, and a random variable X denoting the severity of losses in our context, the Value-at-Risk (VaR) of X at level q (or the $(1-q)$-quantile) is denoted by $VaR_q(X)$ and defined as: $VaR_q(X) = \inf\{z \in \mathbf{R} : P(X > z) \leq q\}$, where $\mathbf{R}$ denotes the real line. This quantity denotes an amount (the VaR), such that the likelihood of losing more than this amount is no more than some tolerance q (e.g., 1%). For this reason the literature is generally interested in the regime $q \leq 1/2$. The also commonly used alternative risk measure, conditional VaR (the average of worst losses - also called expected shortfall or Average VaR), or CVaR, is coherent by the above definition. However, CVaR is the *average* of the worst losses of a (cyber-risk) portfolio (i.e., for $q \in (0,1]$, $CVaR_q(Y) = \frac{1}{q}\int_{1-q}^{1} VaR_{1-\tau}(Y)d\tau$), and subsequently requires existence of the statistical first moments of the loss distribution, which may not be true of catastrophic cyber-risks. For this reason we will limit ourselves to the VaR measure in this paper.

2.2 Mathematically Stable Distributions and Their Convolutions

A distribution is said to be *stable* if a linear combination of two independent random variables with this distribution has the same distribution, up to location and scale parameters (Uchaikin and Zolotarev 2011; Zolotarev 1986; Bouchaud and Potters 2003). The *Normal*, *Cauchy* and the *Levy* distributions are the only stable distributions for which closed form expressions exist, and consequently are often used in analysis for their tractability. Of these three, Cauchy and Levy are heavy-tailed; they are also stable for $\alpha \in (0,2)$. Here α reflects the nature of distributional tails that decline parametrically as a polynomial function of some $\alpha > 0$. Such distributions have finite statistical moments $\mathrm{E}[|X|^p]$ if the order $p < \alpha$, and infinite statistical moments for $p \geq \alpha$. Another attractive property with respect to heavy-tailed stable distributions is the applicability of the central limit theorem for such (non) IID random variables with undefined variance. This generalization (due to Gnedenko and Kolmogorov (Zolotarev 1986)) states that the sum of a number of random variables with symmetric distributions with infinite variances and having power-law tails (Paretian tails), will tend to a stable distribution as the number of summands increase. Specifically, we will denote by $S_\alpha(\sigma,\beta,\mu)$, $0 < \alpha \leq 2$, the distribution of a stable, heavy-tailed r.v. X. Here α is also referred to as the characteristic exponent (or index of stability, which characterizes the heaviness or the rate of decay of the tail); $\sigma > 0$ is the scale parameter, which is a generalization of the concept of standard deviation (it coincides with the standard deviation in the special case of Gaussian distributions ($\alpha = 2$)); $\beta \in [-1,1]$ is the symmetry index that characterizes the skewness of the distribution – a stable distributions with $\beta = 0$ are symmetric about the location parameter μ. In what follows, we write $X \sim S_\alpha(\sigma,\beta,\mu)$, if the random variable X has the stable distribution $S_\alpha(\sigma,\beta,\mu)$ (Ibragimov and Walden 2011). Throughout this paper, we will also limited ourselves to the case of $\mu = 0$ without loss of generality.

For $0 \leq r < 2$, we denote by $\overline{\mathscr{CS}}(r)$ the class of cyber-risk distributions which are convolutions of individually symmetric stable cyber-risk distributions $S_\alpha(\sigma,0,0)$ with indices of stability $\alpha \in [r,2)$ and $\sigma > 0$. That is, $\overline{\mathscr{CS}}(r)$ consists of cyber-risk distributions of r.v.'s X for which, with some $k \geq 1, X = Y_1 + ... + Y_k$, where $Y_i, i = 1,...,k$, are independent r.v.'s such that $Y_i \sim S_{\alpha_i}(\sigma_i,0,0)$, $\alpha_i \in [r,2), \sigma_i > 0, i = 1,...,k$. For $0 \leq r \leq 2$, we denote by $\underline{\mathscr{CS}}(r)$ the class of cyber-risk distributions which are convolutions of individually symmetric and stable cyber-risk distributions $S_{\alpha_i}(\sigma_i,0,0)$ with indices of stability $\alpha_i \in (0,r)$ and $\sigma_i > 0$. That is, $\underline{\mathscr{CS}}(r)$ consists of cyber-risk distributions of r.v.'s X for which, with some $k \geq 1, X = Y_1 + ... + Y_k$, where $Y_i, i = 1,...,k$, are independent r.v.'s such that $Y_i \sim S_{\alpha_i}(\sigma_i,0,0)$, $\alpha_i \in (0,r), \sigma_i > 0, i = 1,...,k$. The

classes $\overline{\mathscr{CS}}(r)$ and $\underline{\mathscr{CS}}(r)$ are mathematically *closed* under convolutions - *a powerful property contributing to tractable analysis of cyber-risks in these families.* A linear combination of independent stable r.v.'s with the same characteristic exponent α also has a stable distribution with the same α. However, in general, this does not hold in the case of convolutions of stable distributions with different indices of stability. Therefore, the class $\overline{\mathscr{CS}}(r)$ of convolutions of symmetric stable distributions with different indices of stability $\alpha \in (r,2]$ is wider than the class of all symmetric stable distributions $S_\alpha(\sigma,0,0)$ with $\alpha \in (r,2]$ and $\sigma > 0$. Similarly, the class $\underline{\mathscr{CS}}(r)$ is wider than the class of all symmetric stable distributions $S_\alpha(\sigma,0,0)$ with $\alpha \in (0,r)$ and $\sigma > 0$.

2.3 Background on Majorization Theory

A vector with n components $w \in \mathbf{R}^n_+$ is said to be majorized by a vector $v \in \mathbf{R}^n$, written as $w \prec v$, if $\sum_{i=1}^k w_{[i]} \leq \sum_{i=1}^k v_{[i]}$, $k = 1, \cdots, n-1$, and $\sum_{i=1}^n a_{[i]} = \sum_{i=1}^n b_{[i]}$, where $w_{[1]} \geq \cdots \geq w_{[n]}$ and $v_{[1]} \geq \cdots \geq v_{[n]}$ denote the elements of w and v in decreasing order, respectively. The relation $w \prec v$ implies that the components of w are *less* diverse than those of v (see (Marshall et al. 1974)). For instance, it is easy to see that the following holds:

$$\left(\sum_{i=1}^n \frac{w_i}{n}, \cdots, \sum_{i=1}^n \frac{w_i}{n}\right) \prec (w_1, \cdots, w_n) \prec \left(\sum_{i=1}^n w_i, 0, ...0\right), \ \forall w \in \mathbf{R}^n_+ \ .$$

It is also immediate that if $w \prec v$, then the same is true for their respective permutations: $(w_{\pi(1)}, \cdots, w_{\pi(n)}) \prec (v_{\pi(1)}, \cdots, v_{\pi(n)})$ for all permutations π of the set $\{1., .., n\}$. A function $\phi : \mathbf{R}^n_+ \to \mathbf{R}$ is called *Schur-convex* (resp. *Schur-concave*) (Boyd and Vandenberghe 2004) if $(w \prec v) \implies (\phi(w) \leq \phi(v))$ (resp. $(w \succ v) \implies (\phi(w) \geq \phi(v))$), $\forall w, v \in \mathbf{R}^n_+$. If the inequalities are strict whenever $a \prec b$ and a is not a permutation of b, then ϕ is said to be strictly Schur-convex (resp. strictly Schur-concave). Evidently, if $\phi : \mathbf{R}^n_+ \to \mathbf{R}$ is Schur-convex or Schur-concave, then $\forall w \in \mathbf{R}^n_+$, we have:

$$\phi(w_1, \cdots, w_n) = \phi(w_{\pi(1)}, \cdots, w_\pi(n)),$$

where π is any permutation of the set $\{1, ..., n\}$. Examples of strictly Schur-convex functions $\phi : \mathbf{R}^n_+ \to \mathbf{R}$ are given by $\phi_\alpha(w_1, \cdots, w_n) = \sum_{i=1}^n w_i^\alpha$ for $\alpha > 1$. The functions $\phi_\alpha(w_1, \cdots, w_n)$ are strictly Schur-concave for $\alpha < 1$ (see Proposition 3.C.1.a in (Marshall et al. 1979)).

To illustrate the above concept via an example, consider a portfolio of cyber-risks $X_1, ..., X_n$ with weights $w = (w_1, ..., w_n) \in \mathbf{R}^+_n$ denoting the fraction of each risk the portfolio is exposed to, i.e., the fraction of each risk an insurer is responsible for covering. The aggregate risk is denoted by $Z_\mathbf{w} = \sum_{i=1}^n w_i X_i$. Denote by $\mathscr{I}_n = \{w = (w_1, ..., w_n) : w_i \geq 0, i = 1, \cdots, n, \sum_{i=1}^n w_i = 1\}$ the simplex of all vectors where weights sum to 1. Define two special vectors $\underline{w} = (\frac{1}{n}, \frac{1}{n}, ... \frac{1}{n}) \in \mathscr{I}_n$ and $\overline{w} = (1, 0, ..., 0) \in \mathscr{I}_n$. Given the same set of risks, the theory of majorization suggests that $\underline{w} \prec \overline{w}$, and a portfolio based on the latter weights is more diverse. This notion of diversity is in a way the opposite of what one might consider to be the variability among the weights: the more diverse $\overline{w}$ has the least varied weights (consisting of a single risk) within $\mathscr{I}_n$, while the less diverse $\underline{w}$ has more varied weights (equally spread over n risks).

3 ANALYZING SYSTEMIC CYBER RISK DIVERSIFICATION SUSTAINABILITY

In this section, we propose the first general theory (to the best of knowledge) to classify the types of cyber risk portfolios that are always diversification-sustainable for cyber insurers with respect to the VaR measure, and portfolios that are not diversification-sustainable.

One of the key features for cyber (re-)insurance to be a scalable business model is its ability to pool cyber risk distributions from multiple enterprises, thereby reducing an underwriter's overall risk exposure. This is particularly true for a reinsurer, who is in a position to significantly diversify its risks, by selling reinsurance to very different front-line insurers who specialize in different sectors (e.g., retail,

pharmaceutical, manufacturing, etc.) in the financial market. Such risks per enterprise also incorporate loss impact shocks from cyber incidents that are targeted at other enterprises in the interconnected IT-driven enterprise ecosystem. Examples of such shocks include IT-driven supply chain disruptions. The metric for decision making for a cyber (re-)insurer here is the VaR of a portfolio post diversification and whether it less than that when compared to cyber risk non-diversification, i.e., specialization. To this end, we have the following major result of our paper showcasing conditions for cyber risk diversification sustainablity, and that is motivated by seminal theory in (Andrews 2005; Ibragimov and Walden 2007; Ibragimov 2009).

Theorem 1 *Consider a cyber insurance firm (including a cyber re-insurance firm) on the verge of decision making regarding diversification of a portfolio of (systemic) cyber risks it is exposed to from an IT-driven enterprise ecosystem that includes supply chain relationships among the enterprises.*

1. *Denote $\overline{\mathscr{CSLC}}$ to be the family of convolutions of symmetric cyber risk distributions that are either from the log-concave (exhibiting atmost an exponential tail risk) family $\mathscr{LC}$ or from the family $\overline{\mathscr{CS}}(1)$. Consider i.i.d. r.v's $X_i \sim \overline{\mathscr{CSLC}}, i = 1, \cdots, n$, $q \in (0, \frac{1}{2})$ forming a cyber risk portfolio, and vector of weights $w, v \in \mathbf{R}^n_+$ of dimension n with the weights in each portfolio summing to 1. Then $VaR_q(Z_w) \leq VaR_q(Z_v)$ if v is not a permutation of w and $v \prec w$ (v is less diverse than w); in other words, the strict Schur-convexity of function $VaR_q(Z_w)$ in $w \in \mathbf{R}^n_+$ holds. In particular, $VaR_q(Z_{\bar{w}}) \leq VaR_q(Z_w) \leq VaR_q(Z_{\underline{w}})$, $\forall w \in \mathscr{I}_n$ such that $w \neq \underline{w}$; w is not a permutation of $\bar{w}$.*
2. *Denote $\underline{\mathscr{CS}}(1)$ to be the family of convolutions of symmetric cyber risk distributions that are from the family cyber risk distributions with infinite mean and variance (i.e., the family of extremely heavy tailed cyber risks). Consider i.i.d. r.v's $X_i \sim \underline{\mathscr{CS}}(1), i = 1, \cdots, n$, $q \in (0, \frac{1}{2})$ forming a cyber risk portfolio, and vector of weights $w, v \in \mathbf{R}^n_+$ of dimension n with the weights in each portfolio summing to 1. Then $VaR_q(Z_w) \geq VaR_q(Z_v)$ if v is not a permutation of w and $v \prec w$ (v is less diverse than w); in other words, the strict Schur-concavity of function $VaR_q(Z_w)$ in $w \in \mathbf{R}^n_+$ holds. Hence, $VaR_q(Z_{\bar{w}}) \leq VaR_q(Z_w) \leq VaR_q(Z_{\underline{w}})$, $\forall w \in \mathscr{I}_n$; $w \neq \underline{w}$; w is not a permutation of $\bar{w}$.*
3. *Consider individual non i.i.d. enterprise pair distributions (arising from IT-driven supply chain disruptions due to a cyber attack on the chain) A_i and B_j for any enterprise pair (i, j) - reflecting individual cyber risk for i and j, with A_i and $B_j \sim \overline{\mathscr{CSLC}}, q \in (0, \frac{1}{2})$ forming a cyber risk portfolio, and n^2-vector of weights $w_{ab}, v_{ab} \in \mathbf{R}^{n^2}_+$ with the weights in each portfolio summing to 1. Then $VaR_q(Z_{\underline{w}_{ab}}) \leq VaR_q(Z_w) \leq VaR_q(Z_{\bar{w}_{ab}})$, $\forall w \in \mathscr{I}_{ab}$.*
4. *Consider individual non i.i.d. enterprise pair distributions (arising from supply chain disruptions) A_i and B_j for any enterprise pair (i, j) - reflecting individual cyber risk for i and j with A_i and $B_j \sim \underline{\mathscr{CS}}(1), q \in (0, \frac{1}{2})$ forming a cyber risk portfolio, and n^2-vector of weights $w_{ab}, v_{ab} \in \mathbf{R}^{n^2}_+$ with the weights in each portfolio summing to 1. Then $VaR_q(Z_{\underline{w}_{ab}}) \geq VaR_q(Z_w) \geq VaR_q(Z_{\bar{w}_{ab}})$, $\forall w \in \mathscr{I}_{ab}$.*

In summary, (systemic) cyber risk portfolios characterized in parts 1 and 3 above are diversification-sustainable. Whereas, cyber risk portfolios in parts 2 and 4 are not diversification-sustainable.

Proof Sketch - The proof for the first two cases revolves around working with the positive homogeneity property of the VaR measure. This property states that $\mathscr{F}(\lambda X) = \lambda \mathscr{F}(X)$ for all $X \in \mathscr{X}$ and any $\lambda \geq 0$. In our theorem, it implies that $VaR_q(Z_v) = (\sum_{i=1}^n v_i^\alpha)^{1/\alpha} VaR_q(X_1)$. Using the Schur-convex and Schur concave properties of $h(v_1, \ldots, v_n) = \sum_{i=1}^n v_i^\alpha$ from Proposition 3.C.1.a in (Marshall, Olkin, and Arnold 1979), we arrive at the results for parts 1 and 2 of Theorem 1. The proof for the last two cases rely upon the application of majorization theory from Lemma 13.B.2 in (Marshall et al. 1979) in addition to application of Theorem 4.1 in (Ibragimov and Walden 2011) inspired from (Andrews 2005).

Practical Implications of the Theorem - The theorem states that a portfolio of cyber risks consisting of (non) i.i.d., light-tailed and moderately heavy-tailed risks with finite mean is diversification-sustainable as the VaR on diversification monotonically decreases when compared to specialization. The contrary holds when a portfolio consists of (non) i.i.d extremely heavy tailed cyber risks with infinite mean and variance - such portfolios are not diversification-sustainable as the VaR on diversification monotonically increases

when compared to specialization. The non i.i.d. nature of the (systemic) cyber risks usually arises from the supply chain disruptions in the IT-driven enterprise ecosystem. Here, as examples, moderate data breach events will induce light-tailed cyber risks whereas local power grid failures for hours due to a cyber attack will induce moderate heavy-tailed risks. A cyber-driven AWS non-availability for hours/days or a US power grid failure will induce extremely heavy-tailed cyber risks.

4 HOW TO MAKE NON-SUSTAINABLE DIVERSIFICATION SUSTAINABLE?

In the previous section, we faced a challenge wherein a cyber insurance company will find it non-sustainable to diversify a portfolio consisting of (systemic) cyber risks having extreme heavy-tailed nature, they being i.i.d., or otherwise. However, the future cyber terrain promises the realistic occurrence of such cyber risk types, and it is desired that a solution is available to effectively manage such risks. *We propose a policy solution backed by provable math that can guarantee the existence of sustainably diversifiable cyber risk portfolios consisting of extremely heavy-tailed cyber risks with infinite mean and variance.*

We assume that heavy-tailed cyber risk distributions (moderate or extreme), denoted by $f(\cdot) \in RV_\gamma$, are measurable functions having a regular variation (RV) with respect to an index γ (Resnick 2008) at $t = 0^+$ or at $t = \infty$. For such functions, $\lim_{t\to t_0} \frac{f(st)}{f(t)} = s^\gamma$, for all $s > 0$. Such distribution functions popularly generalize the power law that usually characterize heavy-tailed distributions. In this section, we assume, as a conservative portfolio, cyber risk r.v.'s X_i to be identical (not independent) with distribution function F and consequently the survival function $\bar{F}$, where $\bar{F} \in RV_{-\alpha}$; $\alpha \leq 1$ to represent extremely heavy-tailed systemic catastrophic cyber risk.

We model the dependency between the (heavy-tailed) risks of a portfolio by the *Archimedean* copula family that covers a wide range of dependence from independence to comonotonicity, and includes the popular *Clayton*, *Gumbel*, and *Frank* copulas (McNeil et al. 2015). An Archimedean copula, for r.v.'s $X_1, \ldots, X_n$ is defined as $C(u_1, \ldots, u_n] = \phi^{-1}(\phi(u_1 + \ldots + \phi(u_n))$, where the generator function $\phi : [0,1] \to [0,\infty]$ is continuous, decreasing, and convex with $\phi(1) = 0, \phi(0) = \infty$; and ϕ^{-1} is completely monotonic to ensure that C is a copula for $n \geq 2$. Now the joint tail probabilities of the cyber risks $X_1 \ldots X_n$ (that accounts for their dependence also) in a portfolio can be modeled using an Archimedean survival copula as $\mathbb{P}(X_1 > x_1, \ldots, X_n > x_n) = \vec{C}(\bar{F}_1(x_1), \ldots, \bar{F}_n(x_n))$, where $\vec{C}$ is the survival copula, with $\phi \in RV_{-\beta}(0^+)$ being a regularly varying function with $\beta > 0$. When β is high, the dependencies among the cyber risks in the portfolio is high and extreme systemic events can occur together. The opposite holds true with extreme systemic risks occurring independently when β is close to zero.

We model the decision construct *price of cyber risk diversification* (POCD) for an insurer portfolio of identical (but non independent) cyber risks as

$$POCD_{q\in(0,1)}(X(k)) = \frac{VaR_q(S_n(k))}{VaR_q(X_1(k))},$$

where $S_n = \frac{1}{n}(X_1(k) + \ldots + X_n(k))$, and k is the upper limit of insurer liability. The bone of contention is extreme heavy-tailed cyber risks, and so we study the diversification effect when $q \to 1$. Cyber risk portfolio diversification will be preferred only if $\lim_{q\to 1} POCD_q(X(k)) \leq 1$ (when $VaR_q(S_n(k)) \leq VaR_q(X_1(k))$) , and not preferred if $\lim_{q\to 1} POCD_q(X(k)) \geq 1$. We have the following theorem, adapted from the general quantitative risk management theory in (McNeil et al. 2015; Embrechts et al. 2009; Cui et al. 2021), on conditions that can make a portfolio of extremely heavy-tailed cyber risks diversification-sustainable.

Theorem 2 *Consider a insurer cyber risk baseline portfolio consisting of n extremely heavy-tailed risks* $X = [X_1, \ldots X_n]$ *with each having continuous distribution function F with* $\bar{F} \in RV_{-\alpha}$ *where* $\alpha \in (0,1]$ *and the dependencies between these cyber risks follow an Archimedean survival copula with* $\phi \in RV_{-\beta}(0^+)$*;* $\beta > 0$*. Assume that there are atleast n cyber insurers in the cyber risk diversification market. Also assume that* $\lim_{q\to 1} \frac{k(q)}{VaR_q(X_1)} = c > 0$*. In such a case we have (i) extremely heavy-tailed cyber risk portfolio*

diversification is sustainable if $c \in (0,n)$ *and* $POCD_q(X(k)) \leq 1$*, and (ii) extremely heavy-tailed cyber risk portfolio diversification is non-sustainable if* $c \in (n,\infty)$ *and* $POCD_q(X(k)) \geq 1$.

Proof Sketch - Observe that $VaR_q(S_n(k)) \leq k$ for any q. It immediately follows that for all $q_0 < q < 1$, $POCD_q(X(k)) \leq 1$. Now for $c > 1$, we need to study if $\lim_{t\to\infty} \frac{\mathbb{P}(S_n(k)>t)}{\mathbb{P}(X_1(k)>t)} \leq 1$. This involves manipulating algebra using the seminal inclusion-exclusion principle and Proposition 2.2 in (Embrechts et al. 2009) to derive $\lim_{t\to\infty} \frac{\mathbb{P}(S_n>t)}{\mathbb{P}(X_1>t)} = \lim_{t\to\infty} \frac{\mathbb{P}(S_n>t)}{\mathbb{P}(nS_n>t)} \frac{\mathbb{P}(nS_n>t)}{\mathbb{P}(X_1>t)} = n^{-\alpha} q_n(\alpha,\beta)$, where $nS_n \in RV_{-\alpha}$. We are then left to show that $\lim_{t\to\infty} \frac{\mathbb{P}(S_n>t)}{\mathbb{P}(X_1>t)} \leq 1$ that we can show using the notion of supermodular ordering as in (Cui et al. 2021). When $c > n$, a similar algebraic analysis can show that $\lim_{t\to\infty} \frac{\mathbb{P}(S_n>t)}{\mathbb{P}(X_1>t)} = q_n(\alpha,\beta)n^{-\alpha} \geq 1$.

Practical Implications of the Theorem - In conditions when the liability limit k is high enough for a cyber insurer for an enterprise in comparison to the *VaR* of the exposed risk for that enterprise, the diversification of such a portfolio of cyber risks is not sustainable simply because the insurers tend to commit to 'over-coverage' w.r.t. the VaR and make POCD greater than 1. Here, immaterial is the nature of the tail of cyber risks and the extent of their mutual dependencies. In other words, even if $k > n \cdot VaR(X_1)$ (systemic) cyber risks that are not heavy-tailed catastrophic will behave like one for diversification purposes and ensure its non-sustainability. On the other hand, if $k < n \cdot VaR_q(X_1)$ then even heavy-tailed (systemic) cyber risks behave like less heavy-tailed cyber risks and diversification becomes sustainable with POCD becoming less than 1. Alternatively, only if n is high, i.e., $n > \frac{k}{VaR_q(X_1)} = c$, *a large enough number of cyber insurers enables sustainable cyber risk diversification of portfolios with extremely heavy-tailed risks.*

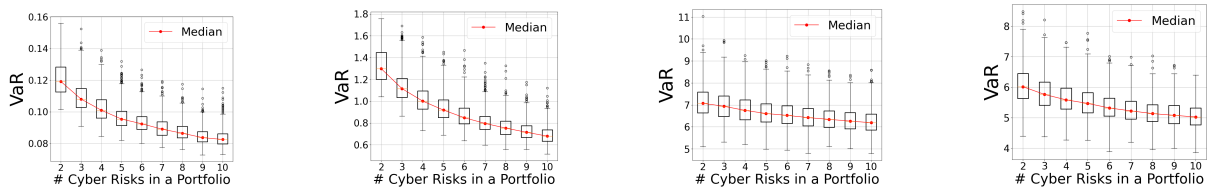
5 NUMERICAL EVALUATION

We conducted large scale Monte Carlo simulations (with 10K runs) to investigate how diversification and specialization (SP) of cyber risk portfolios impact VaR for both i.i.d. and non i.i.d. cyber risk distributions. For each size of the portfolio of such risks, we generated random weights of portfolio cyber risks using a standard Dirichlet distribution, ensuring the portfolio weights sum up to one. VaR at the 95th percentile was calculated for each diversified portfolio. Three types of distributions: Normal, Beta (light-tailed log concave type), and Pareto (heavy-tailed with index parameter between 1 and 2 exhibiting moderately heavy-tailed nature) were used as portfolio risks for simulation purposes. Non-iid risk distributions had manually assigned variances and shape parameters without loss of generality. We study portfolio samples to observe whether *diversification is sustainable* (DIS) or *diversification is not sustainable* (DINS) for such portfolios for i.i.d. and non i.i.d. settings.

The theory in our paper is validated in Figure 1 for a portfolio of *i.i.d.* cyber risks of light-tailed and moderate heavy-tailed distributions, i.e., diversification is sustainable. Figure 2 has two sets of plots: the top two rows, subfigures (a) - (l), indicating *non i.i.d.* Normal (not necessarily mathematically stable) cyber risk distributions and the bottom two rows, subfigures (m) - (x), indicating non i.i.d., Pareto (not necessarily mathematically stable) cyber risk distributions). We observe that to the positive surprise of cyber insurers, diversification is sustainable (DIS) in most situations (MC sample frequency) of general and non-stable (a) Normal cyber risk portfolios, and (b) a significant fraction of all parameter settings of Pareto cyber risk portfolios. However, there exist parameter settings of Pareto portfolios for which only specialization (SP) is sustainable (i.e., DINS - diversification is not sustainable), simply because of the joint condition that more weights are concentrated towards cyber risks with lower Pareto α values (more heavy-tailedness), and the SP portfolio has a higher Pareto α value (less heavy-tailedness).

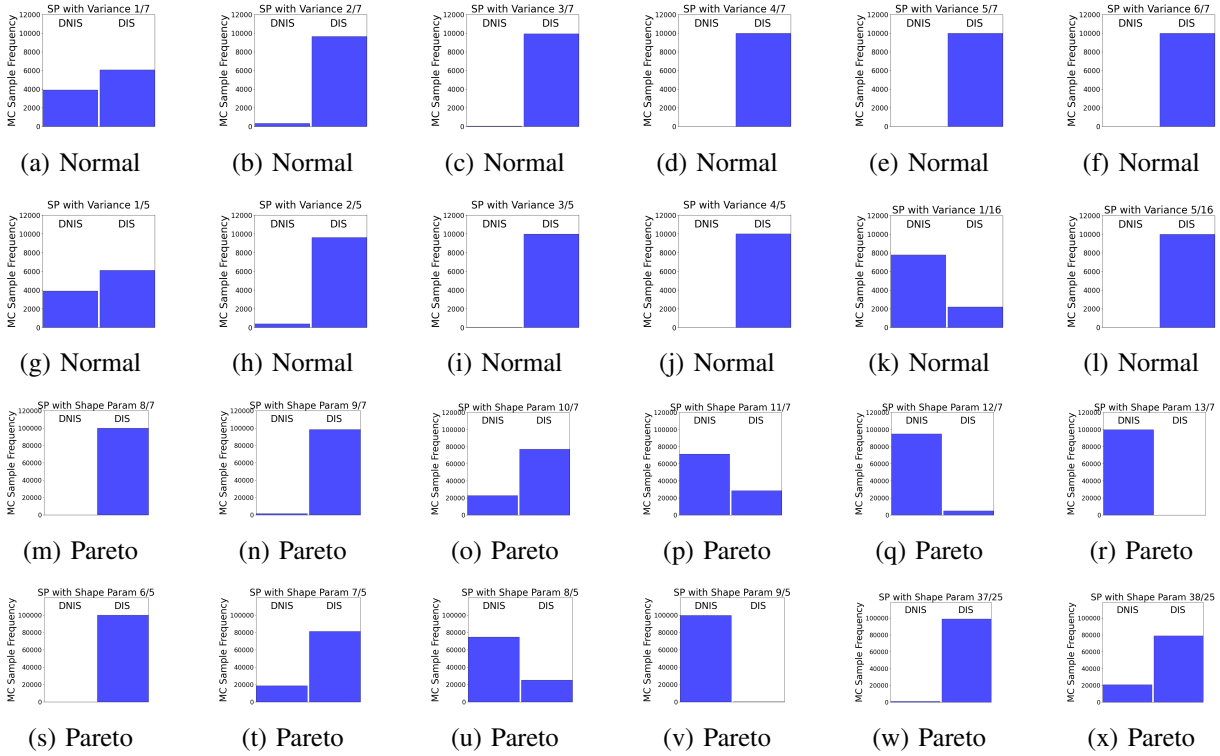
6 RELATED WORK

We review related work in this section in a concise and brief manner in the interest of space. We review existing research related to (a) cyber insurance as a mechanism to improve cybersecurity, (b) computational hardness to diversify (systemic) cyber risk, and (c) cyber risk management on aggregate cyber risk.



(a) Beta $\alpha = 1$ $\beta = 20$ (b) Normal (c) Pareto $\alpha = 1.4$ (d) Pareto $\alpha = 1.5$

Figure 1: Illustrating cyber risk portfolio diversification sustainability for i.i.d. risks with light/heavy tails.



(a) Normal (b) Normal (c) Normal (d) Normal (e) Normal (f) Normal

(g) Normal (h) Normal (i) Normal (j) Normal (k) Normal (l) Normal

(m) Pareto (n) Pareto (o) Pareto (p) Pareto (q) Pareto (r) Pareto

(s) Pareto (t) Pareto (u) Pareto (v) Pareto (w) Pareto (x) Pareto

Figure 2: Illustrating cyber risk portfolio diversification (non) sustainability for non i.i.d. risks with light and heavy tails with portfolio sizes varying between 4 and 6 distributions and varying SP parameters.

The proven potential of cyber-insurance to improve cybersecurity has been mathematically shown in seminal papers (Lelarge and Bolot 2009; N.Shetty et al. 2009; Hoffman 2007; Pal and Golubchik 2010; Pal et al. 2014; Naghizadeh and Liu 2014; Pal et al. 2018; Pal et al. 2011; Pal et al. 2017), though without reaching market efficiency in an economic sense. However, this has not completely discouraged cyber-insurance providers from increasing their supply of solution products, that is steadily seeing an increase over the years (specifically, since the last decade and a half). This is because cyber insurance solutions demand sufficient cybersecurity controls on part of enterprise clients via insurance contracts that consequently supports these enterprises to effectively adapt, absorb, and respond to cyber incidents.

A necessary condition for cyber insurance markets to scale towards being market efficient is for insurers to be able to estimate and consequently diversify (systemic) cyber risk portfolios. In recent related efforts (Pal et al. 2021; Pal et al. 2023), the authors show the optimal cyber-risk diversification problem (a related variant of the optimal systemic cyber-risk estimation problem as optimal risk diversification relies upon optimal systemic cyber-risk estimation as a problem instance) in service networks to be NP-Hard for residual cyber-risk managers. The diversification problem assumes that accurate knowledge of security

investment by enterprises organizations is an information asymmetry (IA) challenge, and show that it is NP-hard to design optimal cyber (re-)insurance contracts under the inevitable IA challenge.

However, the hardness of optimally diversifying (systemic) cyber-risk does not deter the existence of non-optimal but diversification sustainable portfolios of (systemic) cyber risk. Recent theoretical efforts investigated the diversification sustainability problem for i.i.d. cyber risk portfolios. In a series of efforts (Pal et al. 2020; Pal et al. 2020; Pal et al. 2020; Pal et al. 2023; Pal et al. 2021), the authors have proved that spreading *catastrophic* heavy-tailed cyber-risks that are identical and independently distributed (i.i.d.), i.e., not tail-dependent, *is not* an effective practice for cyber re-insurers, whereas spreading i.i.d. heavy-tailed cyber-risks that are *not catastrophic* is. *Orthogonal to investigating on the feasibility of diversified cyber re-insurance markets specific to i.i.d portfolios with heavy-tailed cyber risks, we investigate on the feasibility for any general portfolio with and without i.i.d. cyber risks with arbitrary tail natures.*

7 SUMMARY

We solved the theory challenge problem of proposing mathematical conditions on cyber risk distributions that make systemic risk VaR diversification-friendly for cyber insurance markets. We proposed and validated the first mathematically rigorous classification scheme on the sustainability existence of systemic cyber risk management by the cyber insurance industry, for general (i.i.d. and non i.i.d.) systemic cyber risk distributions based on their tail nature. We laid out quantitatively-backed practical implementation measures to ensure sustainable systemic cyber risk management for portfolios comprising these general risk types.

ACKNOWLEDGEMENT

This study has been supported by funding from Cybersecurity at MIT Sloan (CAMS).

REFERENCES

Andrews, D. W. 2005. "Cross-section regression with common shocks". *Econometrica* 73(5):1551–1585.

Bouchaud, J.-P. and M. Potters. 2003. *Theory of Financial Risk and Derivative Pricing: from Statistical Physics to Risk Management*. Cambridge: Cambridge university press.

Boyd, S. and L. Vandenberghe. 2004. *Convex Optimization*. Cambridge: Cambridge university press.

Cui, H., K. S. Tan, and F. Yang. 2021. "Diversification in catastrophe insurance markets". *ASTIN Bulletin: The Journal of the IAA* 51(3):753–778.

Eling, M., M. Elvedi, and G. Falco. 2023. "The economic impact of extreme cyber risk scenarios". *North American Actuarial Journal* 27(3):429–443.

Embrechts, P., J. Nešlehová, and M. V. Wüthrich. 2009. "Additivity properties for Value-at-Risk under Archimedean dependence and heavy-tailedness". *Insurance: Mathematics and Economics* 44(2):164–169.

Hanouz, M. 2016. "Understanding systemic cyber risk-global agenda council on risk and resilience". In *World Economic Forum*.

Hoffman, A. 2007. "Internalizing Externalities of Loss Prevention Through Insurance Monopoly". *Geneva Risk and Insurance Review* 32.

Ibragimov, R. 2009. "Portfolio diversification and value at risk under thick-tailedness". *Quantitative Finance* 9(5):565–580.

Ibragimov, R. and J. Walden. 2007. "The limits of diversification when losses may be large". *Journal of banking & finance* 31(8):2551–2569.

Ibragimov, R. and J. Walden. 2011. "Value at risk and efficiency under dependence and heavy-tailedness: models with common shocks". *Annals of Finance* 7(3):285–318.

Lelarge, M. and J. Bolot. 2009. "Economic incentives to increase security in the internet: The case for insurance". In *IEEE INFOCOM 2009*, 1494–1502. IEEE.

Marshall, A. W., I. Olkin, *et al*. 1974. "Majorization in Multivariate Distributions". *The Annals of Statistics* 2(6):1189–1200.

Marshall, A. W., I. Olkin, and B. C. Arnold. 1979. *Inequalities: Theory of Majorization and its Applications*, Volume 143. New York: Springer.

McNeil, A. J., R. Frey, and P. Embrechts. 2015. *Quantitative risk management: concepts, techniques and tools-revised edition*. Princeton university press.

Naghizadeh, P. and M. Liu. 2014. "Voluntary participation in cyber-insurance markets". In *Workshop on the Economics of Information Security (WEIS)*.

N.Shetty, G.Schwarz, M.Feleghyazi, and J.Walrand. 2009. "Competitive Cyber-Insurance and Internet Security". In *WEIS*.

Pal, R. and L. Golubchik. 2010. "Analyzing self-defense investments in internet security under cyber-insurance coverage". In *2010 IEEE 30th International Conference on Distributed Computing Systems*, 339–347. IEEE.

Pal, R., L. Golubchik, and K. Psounis. 2011. "Aegis a novel cyber-insurance model". In *International Conference on Decision and Game Theory for Security*, 131–150. Springer.

Pal, R., L. Golubchik, K. Psounis, and P. Hui. 2014. "Will cyber-insurance improve network security? A market analysis". In *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*, 235–243. IEEE.

Pal, R., L. Golubchik, K. Psounis, and P. Hui. 2017. "Security Pricing as Enabler of Cyber-Insurance A First Look at Differentiated Pricing Markets". *IEEE Transactions on Dependable and Secure Computing*.

Pal, R., L. Golubchik, K. Psounis, and P. Hui. 2018. "Improving Cyber-Security via Profitable Insurance Markets". *ACM SIGMETRICS Performance Evaluation Review* 45(4):7–15.

Pal, R., Z. Huang, S. Lototsky, X. Yin, M. Liu, J. Crowcroft, , *et al*. 2021. "Will Catastrophic Cyber-Risk Aggregation Thrive in the IoT Age? A Cautionary Economics Tale for (Re-) Insurers and Likes". *ACM Transactions on Management Information Systems (TMIS)* 12(2):1–36.

Pal, R., Z. Huang, X. Yin, M. Liu, S. Lototsky and J. Crowcroft. 2020. "Sustainable catastrophic cyber-risk management in IoT societies". In *2020 Winter Simulation Conference (WSC)*, 3105–3116. IEEE.

Pal, R., Z. Huang, X. Yin, S. Lototsky, S. De, S. Tarkoma, , *et al*. 2020. "Aggregate Cyber-Risk Management in the IoT Age: Cautionary Statistics for (Re) Insurers and Likes". *IEEE Internet of Things Journal* 8(9).

Pal, R., P. Liu, T. Lu, and E. Hua. 2023. "How Hard Is Cyber-risk Management in IT/OT Systems? A Theory to Classify and Conquer Hardness of Insuring ICSs". *ACM Transactions on Cyber-Physical Systems (TCPS)* 6(4):1–31.

Pal, R., P. Liu, T. Lu, and X. Yin. 2021. "Cyber Re-Insurance Policy Writing is NP-Hard in IoT Societies". In *2021 Winter Simulation Conference (WSC)*. IEEE.

Pal, R., K. Psounis, J. Crowcroft, F. Kelly, P. Hui, S. Tarkoma, , , , *et al*. 2020. "When Are Cyber Blackouts in Modern Service Networks Likely? A Network Oblivious Theory on Cyber (Re) Insurance Feasibility". *ACM Transactions on Management Information Systems (TMIS)* 11(2):1–38.

Resnick, S. I. 2008. *Extreme values, regular variation, and point processes*, Volume 4. Springer Science & Business Media.

Uchaikin, V. V. and V. M. Zolotarev. 2011. *Chance and Stability: Stable Distributions and their Applications*. Berlin: Walter de Gruyter.

Welburn, J. W. and A. M. Strong. 2022. "Systemic cyber risk and aggregate impacts". *Risk Analysis* 42(8):1606–1622.

Zolotarev, V. M. 1986. *One-dimensional Stable Distributions*, Volume 65. Providence: American Mathematical Soc.

AUTHOR BIOGRAPHIES

RANJAN PAL is a Research Scientist with the MIT Sloan School of Management, and an invited working group member of the World Economic Forum. His primary research interest lies in developing interdisciplinary cyber risk/resilience management solutions. He serves as an Associate Editor of the ACM Transactions on MIS. His email address is ranjanp@mit.edu.

KONNIE DUAN is a student in the Electrical Engineering and Computer Science (EECS) department at MIT. She is also a researcher with Cybersecurity at MIT Sloan (CAMS) at the MIT Sloan School of Management. Her primary research interest lies in cyber and financial risk management for business enterprise ecosystems. Her email address is konnie@mit.edu.

ROHAN XAVIER SEQUEIRA is a PhD student and an Annenberg Fellow in the Electrical and Computer Engineering (ECE) department at the University of Southern California. His research interest lies is cyber-risk management, privacy, and distributed systems. His email address is rsequeir@usc.edu. Rohan got his MS in ECE from the University of Michigan Ann Arbor.

MICHAEL SIEGEL is a Principal Research Scientist with the MIT Sloan School of Management. His primary research interest lies in cyber-security management of information systems. He is the founding co-Director of the Cybersecurity at MIT Sloan (CAMS) center within the MIT Sloan School of Management. His email is msiegel@mit.edu.